

User Guide

VirusBuster Scanner

for Windows/Linux/OpenBSD/FreeBSD/Solaris/AIX



TABLE OF CONTENTS

VIRUSBUSTER SCANNER	3
System requirements	3
Functionality	5
Options	5
Some examples	11
Scheduled launching (only on Linux/Unix systems).....	13
Returned values.....	13
The configuration file	14
Virus database updating	15
 END USER AGREEMENT	 16
 CONTACT	 17

VIRUSBUSTER SCANNER

The VirusBuster Scanner programs have been drawn together in this manual, as they are similar and have same functionality. The differences in the operation of the programs will be indicated. The task of the VirusBuster Scanner programs is to find virus infections on the data storage systems and other areas and if possible remove them. The program provides the opportunity for performing regular scans on the data storage devices. The program can be run from the command line and its operation can be adjusted with aid of parameters. An automatic protection can be achieved, to a certain degree, by using the parameters.

Main features of the product:

- Operating in interactive and automatic modes
- Heuristics scanning levels
- Multi-thread scanning
- Enable/disable boot scanning
- Option's values can be stored in configuration file
- Command line quarantine handling
- Incremental virus database update

System requirements

The following system requirements must be available to execute the program:

General requirements

x86, amd64, ia64 processor at 200 MHz minimum

64 MB of RAM

40 MB of free hard disk space

Supported platforms

WINDOWS: 95/98/Me/NT4/NT4s/2000/2000s/XP/XP-x64/2003s/2003s-x64

LINUX GLIBC 2.2.5, kernel 2.2.x (i386, amd64)

FREEBSD 4.9, 5.4, 6.0 (i386) and 6.0 (amd64)

OPENBSD 3.4, 3.6 (i386)

SOLARIS 9 / SunOs 5.9 (sparc)

UltraSparc IIe at 500 MHz

128 MB memory

AIX 4.3, 5.2 (powerpc)

Maintenance level 10

Power3 - II (G3)

256 MB memory

Package naming



vbscan-<productversion>-<platform>[version].tar.gz

Functionality

The VirusBuster Scanner applications act as command line scanners, they scans the system for viruses by options specified in the command line or in the configuration file. It is possible to store the general settings in a configuration file so only your extra settings should be specified in the command line when required. The multi-thread operation provides faster scanning using parallel processing.

The modules of the VirusBuster Scanner program can be found in a simple archived file, you have to unpack them before use. The package contains the following modules:

vbscan.exe | vbscan

Main executable file (on Windows | Unix systems)

vbeng*.dll | libvbengine.so

Scan engine module (on Windows | Unix systems) on the other systems the main executable file

includes this module.

vbscan.ini

Configuration file

vdb/

Folder storing the virus database files

docs/<lang>/

Contains:

- Description of the program
(in text and man page (Unix) format)
- End user license agreement

Use the vbscan.exe or vbscan file to launch scanning, the settings can be specified in the program's configuration file or by command line options.

Important!

The presence of previous version(s) of VirusBuster products in the system can have an effect on the scanner so you should uninstall it/them if there is any problem with the product!

If the location of the configuration file is not specified in the command line, then the program is searching for it automatically and tries loading it from the current directory or the program's home directory (where the executed main program file is found). If the configuration file is not found only the command line options will be applied.

You will not be able to launch the program if the required settings are not specified either in the configuration file or in the command line.

Before scanning you are required to set the quarantine directory (-y option), the temporary directory (-t option) and also recommended the location of virus database (-d option).

Options

Options are divided into groups for best lucidity. We were about to using standard tags and the frequently used ones can be specified by short option names as well. The default settings are indicated at the required topics, these functions are activated without specifying any options.

Information

-V --version

Prints the program's version number then exits.

**-h --help**

Prints the general command line options, their default values and the application's version number.

--full-help

Prints all the command line options, their default values and the application's version number.

Registration data

-k --registration-key

Specifying the registration key based on your license. The program handles the hyphen separated form, too (XXXXX-XXXXX-XXXXX).

-u --registered-user

Specifying the user name based on your license.

Using program without - valid - registration data you have to wait 30 seconds after starting scanner. You have to specify both the registration key and the user name for successfully registration.

Operational settings

--terse

Enables compact log mode.

Compact mode:

/mnt/test/eicar.zip//eicar1.com: found: EICAR skipped.

Original mode:

/mnt/test/eicar.zip//eicar1.com

virus found: EICAR_test_file (NOT killable) ... skipped.

-q --quiet

Enables the quiet working method. The program displays only the virus incidents on the screen or in the log file and a summarized statistics at the end of the scan.

Duplicate use:

-qq or --quiet --quiet

This time the program writes out just the virus incidents to the stdout, summarized statistics also skipped.

Triple use:

-qqq or --quiet -quiet --quiet

Combines the effect of --terse and -qq options.

IMPORTANT! 'quiet' option affects only the stdout, error messages could be returned by stderr.

--summary

Disables displaying summarized statistics tables about the scan.

If -qq or --quiet --quiet options are also specified, it results reversed action: enables the summary display.

-o --old

The program doesn't show warning message if virus database is older than two weeks.

-c --config=FILE

Specifying the used configuration file with its path. If this option is not set, the program is looking for that file (named vbscan.ini by default) in the actual folder. If that one doesn't contain the .ini file the program's home directory will also be scanned for it. The configuration file is suitable for storing common settings needed for a general scanning. These settings can be redefined by command line options if necessary.

Note that the program will try to locate the files and directories that are specified by relative path in the configuration file starting from the actual directory (from which one the program was launched).

-E --engine=FILE

It is possible to set the location of the virus scan engine file to be used. By default, it is used from the program's home folder.

--debug=FILE

If debug file is specified, the program will create it during the scan process to log detailed information about the program operations. It can help you to analyze the scan if necessary.

Scan area settings

-Z --skip-archive

Archived files will not be scanned.

The archived files are scanned by default.

-b --boot

The program scans the computer's boot sectors as well. Impossible to scan boot sectors separately. This option is working only on Windows system.

-M --skip-mail

MIME of type files will not be scanned.

The MIME files scanning is included by default.

--symlink=ACTION

Handling symbolic references (this option is working only on unix systems).

Available values (actions):

follow - uses the link name to identify the file

resolve - uses the file's own name to identify it

(in such a cases, it scans the referenced file as a regular file)

skip - ignores symbolic references

(in such a case it doesn't scan symlinks)

-R --skip-subdir[=PATH]

The program scans each subdirectories recursively by default if a directory is specified as target. If you set this option, you can select directories or directory fragments to exclude from the scan while the other locations will be scanned recursively. If you use this option without parameter (the -R or --skip-subdir alone) then all the subdirectories of the specified target area will be ignored.

-f --file=FILE

Text file containing paths and files (objects) to be scanned. This option's value locates the path of this text file. The objects will be read by lines from the file.

Special parameter: '-' hyphen ('--file=-'): this time the scanner reads the names of the files or directories to scan from STDIN (only in automatic mode).

This option can't be used for scanning quarantine items and boot sectors!

Scanned file types

By default only file types matching any item of the scan engine internal pattern list (default extensions) will be scanned during the virus scan. These are the following:

Program files: *.exe|*.com|*.ov?|*.sys|

.386|.bin|*.dll|*.drv|*.lnk|*.ocx|*.prg|

.scr|.vxd|*.crt|*.prc|*.xml|*.swf

Script files: *.bat|*.ht*|*.js|*.jse|*.vbs|



```
*.ini|*.csc|*.hlp|*.shs|*.pif|*.ade|*.adp|
*.bas|*.chm|*.cmd|*.cpl|*.inf|*.ins|*.isp|
*.zl*|*.mde|*.msc|*.msi|*.msp|*.mst|*.pcd|
*.reg|*.scr|*.sct|*.url|*.vb|*.vbe|*.ws*|
*.ans|*.tmp|*.mpp|*.mpt|*.
```

Document files: *.do?|*.rtf|*.wiz|*.eml

Chart files: *.xl?

Access files: *.mdb

Presentation files: *.ppt|*.pot

Compressed files: *.arj|*.a??|*.zip|*.rar|

.cab|.gz|*.bz2|*.tgz|*.tar|*.dbx

The default pattern values can be altered with the following options:

--all-files

Switches off the pattern matching at all so all file types will be scanned.

-p --pattern=PATTERN

The program scans only that files which match the specified PATTERN.

--include=PATTERN

Adds PATTERN to the default configuration.

--exclude=PATTERN

Excludes PATTERN from the default configuration. This option takes precedence over the above options.

-m --match-in-archive

Pattern-matching inside the archives is enabled by default if you use the built in patterns of the scan engine for scanning (using '--include' and/or '--exclude'). In every other cases it is disabled (using '--pattern' or '--all-files'). This option changes the default value.

Relations:

- '--all-files', '--pattern', '--include' could not be used at the same time
- If you don't specify either of the above options, the program will scan the files with the default extensions

PATTERN syntax:

Several patterns can be specified in the pattern option separated by pipe (|). The pattern can contain ? and * meta-characters (the ? (question mark) is considered as an optional character, the * (star) is considered as an optional character chain). The program is also able to handle character-classes for more restriction. Character-classes must be specified between brackets (e.g. [abc]). The exclamation mark '!' means negation if it is placed straight after the initial bracket '['. The '-' sign placed between two characters means a character range. If you want the '-' or '!' signs to be a considerable character, you should place it straight before the ending bracket ']'. The program does not make a distinction between small and capital letters.

The '*' and '?' meta-characters do not match directory separator characters in pathnames. The special '***' sequence can be used to match any arbitrary characters including directory separators. For example:

'Program Files*.exe' - each .exe file will be matched in the Program Files directory and its subdirectories

Important!

PATTERN is matched against file's basename (filename without path) if PATTERN itself does not contain directory separator characters or '***' sequences, otherwise full path to the file shall be used. The separator character is '/' on Unix and GNU/Linux, and '\' on Windows that is the same as you can use to convert meta characters to literals. The application usually consider '\' as directory separator. It should be used duplicated if special characters follow it. These characters are: | * ? [] .



Scanning methods and actions in case of virus incidents

-e --heuristics = (o | off | n | normal | h | high)

Heuristics level setting. Default: normal level.

o / off - heuristics off

n / normal - normal level

h / high - high level

-s --scanning = (q | quick | s | strict | f | full)

Scanning method setting. Default: regular level.

q / quick - Only scans those parts of the file, which are most likely to contain a virus and does not detect viruses, which can only be detected by using a major amount of system resources (e.g. Excel FORMULA viruses).

s / strict - Optimized scanning method, which detects all viruses registered in the virus database and scans those parts of the file, which are most likely to contain a virus.

f / full - Detects all viruses registered in the virus database and scans the whole file, even those parts, where viruses are not likely to be found.

--thread=NUM

Maximum number of program threads. This option's value is 1 by default. The multi-thread applications result in better performance, but this strongly depends on the system settings.

--timeout=NUM

Timeout limit of the scanning threads (seconds). Scanning will be cancelled if all the threads or just one of them exceed this limit - depending on the '---timeout-abort' option - and have no activity over the specified time-interval. You should increase this limit in case of large archives or strongly loaded system.

--timeout-abort

A '---timeout-abort' option affects the abort mechanism. If this option is set the program will be aborted immediately in case of first timeout.

This function is disabled by default that means the program runs until at least one thread ends within the specified limit.

The default ---thread setting allows only one thread to be run so if it exceeds the timeout the program will be aborted.

-a --action=ACTION

Setting this option the program can be run in automatic mode so the specified action(s) will be performed without user interaction on virus incidents. If the action option is used repeatedly in the command line (separated by commas (,)), the actions will be considered and performed by their order. The first specified action has the highest priority and so on. If the first action can't be performed the following one will be tried. If the action (-a or --action) is not specified at all, the user is asked to choose an action in case of any incidents (interactive mode).

Meaning of the available actions.

k - virus killing from the file (kill)

s - ignores the infected object (skip)

r - renaming the file (rename)

q - moving to quarantine (quarantine)

d - irreversible deleting (delete)

--remove-macro

Automatically deletes all the macros from the Microsoft Office documents without any confirmation.

--sfx

Enables SFX (self extractor) recognition (it may result in scanner performance decrease (about 30% slower scanning)).

--archive-max-size=NUM

Default value: 0 (in such a case, the program is using the virus scan engine's default value).

If this file size limit is exceeded during the decompression of an archive, the program stops this action and also the scan of the file and returns exploit virus found. (Option's value is in MByte).

--archive-max-ratio=NUM

Default value: 0 (in such a case, the program is using the virus scan engine's default value).

Example value: 50

If the size of the decompressed file is 50 times (or more) greater than the compressed file's, the program will return exploit virus found.

Other explanation (option's value in percent): $1/n \times 100$, where n is the value.

In the example: $1/50 \times 100 = 2\%$ so if the compression ratio is better than 2% the program will return exploit virus found.

-G --greyware

If you use this option, the program will detect the applications marked as greyware in the database and perform the specified action on them.

Greyware cannot be clearly categorized as malicious or not malicious application because it strongly depends on its use. Generally this kind of software is not harmful program in case it is installed by the user's consent and approval. But it can happen, that this program is installed in the background without the user's permission and in this case it can be used for malicious activity (for example an ftp server program or a remote access application).

So, in case of greyware, we cannot declare the application as malicious or not malicious based on the name or files of the program, it depends on the method of its installation.

Quarantine handling

The following options can accept one or more KEY(s) or KEY:FILE argument(s), the actions will be performed only on these specified files. If KEY is not specified, the selected action is performed on each file found in quarantine. KEYS belonging to items can be displayed by listing (--list) the contents of the quarantine directory.

--status = (all | clean | deleted | infected | suspicious)

Using this option you can limit/change the default range of quarantine items to be processed. Select the desired value to process only items being in the specified infection status. The 'all' means that the specified action will be applied to all the items.

This option's default value depends on the specified quarantine option:

--list: 'all'

--restore: 'clean'

--delete: 'infected'

--saveas: 'all'

-l --list[=KEY]

Prints the quarantined files with their KEYS, infection status (see the --status option), original location, file size and date of last modification. Use KEY argument to print only the requested items.

--rescan[=KEY]

Rescans the quarantined files or the specified file (in case of using KEY argument). The --status option is ineffective to the --rescan option.

--restore[=KEY[:FILE]]



Restores all the quarantined items or only the specified ones to their original location cleaned by '--rescan' command. Non-existed directories will not be created, existed files will not be rewritten (except when '--overwrite' option is set).

Important!

This option restores only the cleaned, uninfected files by default, but you can override this operation by using the --status option to specify items with different status. Use this option (--status) if you are sure that the item to be restored is not infected.

--delete[=KEY]

Deletes all the quarantined items or only the specified ones from the quarantine. This option deletes only the infected items, you can override this operation by using --status option.

--saveas=KEY:FILE

Saves the specified quarantined file (KEY) which will be named as you wish in the FILE parameter. The item will be saved encoded so the file will not be equal to the original. This function is useful when you would like to send a file to the VirusBuster for analysis.

-w --overwrite

Allows rewriting existing files for '--restore' and '--saveas' operations.

File- and directory references

Non-absolute path name arguments are considered relative to the program's home directory (where the executables are placed).

--log[=FILE]

Screen output could be saved into a specified log file. If file name is not specified (FILE), the output will be appended to the end of a possibly available log file with the default name (vbscan.log).

-y --quarantine=DIR

Specifying the quarantine directory.

-t --temp=DIR

Directory of the temporary files. The TEMP/TMP variable's value is used by default.

-d --vdb=DIR

Specifying the location of the XML descriptor file of the virus database. It is not compulsory to use this option but recommended. If the value of this option is not set, the program will be looking for the virus database in the 'vdb' folder of its home directory.

Some examples

vbscan.exe c:

Scans the whole C: drive and asks the user for further action in case of any incidents.

vbscan.exe --pattern="*.exe|*.dll|*.com" --action=quarantine "C:\Program Files"

Scans Windows binary files in Program Files directory and the infected files will be quarantined to be available for later scanning.

Important!

File names which contain special characters ('space' in this example) must be specified between quotes (" ") on Windows system!



vbscan --pattern='*.exe|*.dll|*.com' --action=quarantine /mnt/windows/c/

Binary files scanning on a mounted Windows partition on Linux. The infected files are to be quarantined automatically.

Important!

Joker characters have to be protected against shell interpreter on Linux/Unix systems so they have to be enclosed in ' ' (single quote) signs!

vbscan.exe --rescan --action=kill --restore --delete

Rescans the quarantine directory's items and try cleaning them. The cleaned items will be restored to their original location with original name. The remaining ones (which can't be disinfected) will be deleted from the quarantine.

vbscan --list --status=suspicious

Only the suspicious items will be listed.

vbscan --saveas=0892342:examine.vbq

The quarantine item which has key number 0892342 will be copied into the actual directory as name as 'examine.vbq'.

vbscan.exe --file=- --action=kill

It reads the names of the files or directories to scan from STDIN (--file), infected files will be cleaned (--action).

vbscan c:\ --skip-subdir="Utils\Arc*" --terse

Scanner will scan the c:\ drive recursively, interactively (action is not specified in the command line) but will not scan any of the directories starting with 'Arc' letters in the 'Utils' folder (--skip-subdir). Compact log is enabled (--terse).

Using short option:

vbscan -b -eh -sf --follow -ak,q /

It is scanning for all the files of the system from the root on the highest level, removes the killable viruses and moves the non killable ones into the quarantine. It recognizes that the '--follow' argument is the abbreviation of '--follow-symlink' and several actions are specified in the argument separated by commas.

Scheduled launching (only on Linux/Unix systems)

Automatic program launching can be realized with the help of 'cron' program. For example if you want the scanner to be launched at 8 pm every evening then register into /etc/crontab:

```
00 20 * * * root <path>vbscan<path>vbscan.ini
```

Returned values

Besides the program displays result of scanning on the screen or in log file it is able to inform users about scanning tasks' results by return values. This feature is useful for getting information in case of scanner is run automatically or scheduled.

There are three different basic return values ('A' case):

0

Suspicious or infected objects were not found.

1

Suspicious or infected objects were found among target objects.

2

The specified actions (--action) were performed successfully on the suspicious or infected objects (except if they were "stop" or "skip").

If errors occur during scanning, the program is not able to check or clean some specified objects completely. The return values can change depending on the errors.

Explanation of the return values:

	In the successfully scanned objects		
	no virus found	virus found and not killed	action performed on infected files
'A' case All the specified target objects are scanned successfully	0 (*)	1 (!)	2 (*)
'B' case Failed to scan all the specified target objects	3 (?)	1 (!)	5 (?)
'C' case Failed to scan all the specified target objects because of system errors	6 (?)	1 (!)	8 (?)
'D' case Failed to scan all the specified target objects for lack of file format support	9 (?)	1 (!)	11 (?)

Legend:

number: the return value itself

(*): after scanning the scanned path is surely virus free

(!): after scanning the scanned path contains infected files

(?): after scanning the scanned path may contain infected files

'B' case:

Some files could not be read because of password protection or they were corrupted or exploit danger. These files may carry malicious codes.

'C' case:

System error during scanning (e.g.: access denied, specified path not found).

After it had been repaired you should retry scanning. The cause of the error may be that the specified files do not exist or the program doesn't have permission to access them. High loaded systems could also result the same error codes.

'D' case:

Some files were not scanned successfully. Although the virus scan engine recognizes their format your current scan engine version doesn't support them. You need to update your scanner program to analyze these files completely.

Higher error codes mean bad parameter specification generally:

255

Invalid command line or configuration file parameters, check them!

254

Failed to run scan engine or the specified virus database does not exist!

253

Bad (incompatible) virus database. Check its version!

252

Failed to start scanning maybe for short system resources!

251

Unable to initialize quarantine! Check the value of '--quarantine' parameter!

250

Program running aborted by external request. (SIGINT, SIGTERM)

Return value is always 0 if quarantine operations could be performed successfully.

The configuration file

The configuration file is line-oriented for simple handling. Each line contains different settings, the option's name is conform to long option names.

You can use both the one character long- and the more character long options without dash ('-' or '--'). The options' values are similar to the command line options. In case of logical options the presence or the lack of the related option specifies if the function is enabled or disabled similar to the command line specification. Comments can be specified after '#' character in a new line or at the end of an opened line.

Virus database updating

The product uses incremental virus database update mechanism to keep the virus database up-to-date. The advantage of this method is that the program doesn't need to download the whole virus database file every time (its size is several MBs) but usually only a small additional database package including the virus signatures processed and released recently. Using this mechanism, the download time is decreased to a minimal level so we can release additional virus database packages several times a day to improve the defense. Users can obtain protection against new malware without spending long time and generating considerable network load for the update. The protection is available almost immediately after the signatures of the newly discovered viruses have been processed in our virus lab.

On Windows system

You can update the virus database manually. Our virus database-set consist of several files. The program stores the database files in the 'vdb' folder. You need to update all the files of the following folder from our FTP server:

`update.virusbuster.hu/pub2006/vbuster/vdb.9/`

Finally replace the old virus database files with the downloaded ones.

On Unix systems

We create a script to automate the update process. Find it in the package named `vdbupdate.sh`.

It is going to download the virus database, copy its files into the correct directory ('vdb' by default). Updating will only be performed, if the database available in the server is newer than one installed on your computer. Otherwise the database will be left unchanged.

Available parameters of the script:

```
-h  print list of valid parameters
-v  verbose output
-t  temporary directory, it must not exist (default $TMPDIR)
-i  directory where to put the new virus database file (default $LIBDIR)
-p  use HTTP instead of the default FTP
```

To run the script, you need the `wget` and `sed` programs! With the help of `cron`, you can schedule the script execution.

END USER AGREEMENT

THIS SOFTWARE END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU AND VirusBuster Ltd. READ IT CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AND USING THE SOFTWARE. IT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. BY INSTALLING AND USING THE SOFTWARE, YOU ARE CONFIRMING YOUR ACCEPTANCE OF THE SOFTWARE AND AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS THEN DO NOT INSTALL THE SOFTWARE.

IMPORTANT NOTICE TO USERS: THE SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

1. Definitions

- (a) "Educational Version" means a version of the Software, so identified, for use by students and faculty of educational institutions only. "Home version" means a version of the Software, so identified, for use by individuals on a single computer at home only. Educational and Home Versions may not be used for, or distributed to any party for, any commercial purpose.
- (b) Henceforward VirusBuster Ltd. means VirusBuster Ltd. and (where interpretable) its suppliers and licensors, if any.
- (c) "Not For Resale (NFR) Version" means a version of the Software, so identified, to be used to review and evaluate the Software, only.
- (d) "Software" means the VirusBuster Ltd. (R) VirusBuster(TM) software program supplied by VirusBuster Ltd. herewith, which may also include documentation, associated media, printed materials, and online and electronic documentation.

2. License

This EULA allows you to:

- (a) Install and use the Software on a single computer; OR install and store the Software on a storage device, such as a network server, used only to run or install the Software on your other computers over an internal network, provided you have a license for each separate computer on which the Software is installed or run from the storage device. A license for the Software may not be shared or used concurrently on different computers.
- (b) Educational and Home Version Only. If you have purchased a license for the Educational and/or the Home Version of the Software, then you may install or store the Software on a storage device, such as a network server, used only to run or install the Software on your other computers over an internal network for use by a total number of concurrent users not to exceed the number of user licenses you have been granted; provided, you agree to implement reasonable controls to ensure that your use of the Software does not exceed the number of licenses you have been granted. You agree that VirusBuster Ltd. may audit your use of the Software for compliance with the EULA at any time, upon reasonable notice.
- (c) Make one copy of the Software in machine-readable form solely for backup purposes. You must reproduce on any such copy all copyright notices and any other proprietary legends on the original copy of the Software.

3. License Restrictions

- (a) Other than as set forth in Section 2, you may not make or distribute copies of the Software, or electronically transfer the Software from one computer to another or over a network.
- (b) You may not decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form.
- (c) You may not sell, rent, lease, transfer or sublicense the Software.
- (d) You may not modify the Software or create derivative works based upon the Software.
- (e) You may not use the Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.
- (f) In the event that you fail to comply with this EULA, VirusBuster Ltd. may terminate the license and you must destroy all copies of the Software.

4. Upgrades

If this copy of the Software is an upgrade from an earlier version of the Software, it is provided to you on a license exchange basis. You agree by your installation and use of this copy of the Software to voluntarily terminate your earlier EULA and that you will not continue to use the earlier version of the Software or transfer it to another person or entity.

5. Ownership

The foregoing license gives you limited rights to use the Software. VirusBuster Ltd. and its suppliers retain all right, title and interest, including all copyrights, in and to the Software and all copies thereof. All rights not specifically granted in this EULA, including International Copyrights, are reserved by VirusBuster Ltd. and its suppliers.

6. LIMITED WARRANTY AND DISCLAIMER

- (a) LIMITED WARRANTY. VirusBuster Ltd. warrants that, for a period of ninety (90) days from the date of delivery (as evidenced by a copy of your receipt) that the physical media on which the Software is furnished will be free from defects in

materials and workmanship under normal use.

(b) NO OTHER WARRANTY. EXCEPT AS SET FORTH IN THE FOREGOING LIMITED WARRANTY, VirusBuster Ltd. AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, OR OTHERWISE INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ALSO, THERE IS NO WARRANTY OF NONINFRINGEMENT, TITLE OR QUIET ENJOYMENT. IF APPLICABLE LAW IMPLIES ANY WARRANTIES WITH RESPECT TO THE SOFTWARE, ALL SUCH WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY. No verbal or written information or advice given by VirusBuster Ltd. its dealers, distributors, agents or employees shall create a warranty or in any way increase the scope of this warranty.

7. Exclusive Remedy

Your exclusive remedy under Section 6 is to return the Software to the place you acquired it, with a copy of your receipt and a description of the problem. VirusBuster Ltd. will use reasonable commercial efforts to supply you with a replacement copy of the Software that substantially conforms to the documentation, provide a replacement for defective media. VirusBuster Ltd. shall have no responsibility if the Software has been altered in any way, if the media has been damaged by accident, abuse or misapplication, or if the failure arises out of use of the Software with other than a recommended hardware configuration.

8. LIMITATION OF LIABILITY.

NEITHER VirusBuster Ltd. NOR ITS SUPPLIERS SHALL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION OR THE LIKE), ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE OR THIS EULA BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF VirusBuster Ltd. OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

9. Basis of Bargain

The Limited Warranty, Exclusive Remedies and Limited Liability set forth above are fundamental elements of the basis of the agreement between VirusBuster Ltd. and you. VirusBuster Ltd. would not be able to provide the Software on an economic basis without such limitations.

10. Consumer End Users Only

The limitations or exclusions of warranties and liability contained in this EULA do not affect or prejudice the statutory rights of a consumer, i.e., a person acquiring goods otherwise than in the course of a business.

11. General Provisions

The internal laws of Hungary shall govern this EULA. This EULA contains the complete agreement between the parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous agreements or understandings, whether oral or written. All questions concerning this EULA shall be directed to VirusBuster Ltd.

VirusBuster and VirusBuster logo are trademarks or registered trademarks of VirusBuster Ltd. in Hungary and/or other countries. Other marks are the properties of their respective owners.

CONTACT

This manual provides comprehensive information on operational of our virus protection product. If you have any additional questions about it or would like to share your experience or proposals with us do not hesitate to contact us! Turn to us with confidence, your demands and remarks will be respected.

Address VirusBuster Ltd.
Budapest 1116,
Vegyesz u. 17-25.
Hungary

Phone (+36) 1 382-7000
Fax (+36) 1 382-7007
Web www.virusbuster.hu
E-mail mail@virusbuster.hu
support@virusbuster.hu